Digital ID (Accreditation) Data Standards 2024

I, Katy Gallagher, Minister for Finance, acting as the Digital ID Data Standards Chair, make the following instrument.

Dated 7 November 2024

Katy Gallagher
Minister for Finance
Digital ID Data Standards Chair

Contents

Chapter 1—Preliminary

1.1 Name

This instrument is the *Digital ID (Accreditation) Data Standards 2024*.

1.2 Commencement

This instrument commences at the same time as the *Digital ID Act 2024* commences.

1.3 Authority

This instrument is made under section 99 of the *Digital ID Act 2024.*

1.4 Definitions

Note 1: A number of expressions used in this instrument are defined in the Act, including the following:

(a) accredited entity;
(b) accredited identity service provider;
(c) authenticator;
(d) biometric information;
(e) digital ID.

Note 2: A number of expressions used in this instrument are defined in the Accreditation Rules, including the following:

(a) biometric matching;
(b) cryptographic key;
(c) eIDVT;
(d) presentation attack instrument;
(e) presentation attack detection;

(1) Expressions defined in the Accreditation Rules have the same meaning in this instrument.

(2) In this instrument:

AACA means an ASD-Approved Cryptographic Algorithm as referred to in the *Guidelines for Cryptography* published by the Australian Signals Directorate.

Note: At the time this instrument was made, the *Guidelines for Cryptography* are located at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography.

Accreditation Rules means the *Digital ID (Accreditation) Rules 2024*.

Act means the *Digital ID Act 2024*.

AE-compromise resistance means authentication protocols that do not require an accredited entity to persistently store secrets that could be used for authentication.

AL Table: see section 3.1.

Section 1.4

APCER means an attack presentation classification error rate.

authentication level: see section 3.1.

authenticated protected channel means a communication channel that uses approved cryptography where the client connection has authenticated to the relevant server.

authentication protocol means a defined sequence of messages between an individual and an ISP where the messages authenticate the individual to their digital ID by demonstrating that the individual has possession and effective control of one or more valid authenticators that have previously been bound to their digital ID.

biometric sample means biometric information that is collected from an individual using a biometric capture device or sensor and is converted into an analogue or digital representation.

biometric testing entity: see subsection 2.2(2).

custom biometric capability means a biometric binding or authentication capability integrated with the entity's accredited services that is distinct from an in-device biometric capability.

document liveness means the presence of the original physical photo ID credential.

false match rate has the same meaning as in ISO/IEC 2382-37: 2022.

false non-match rate has the same meaning as in ISO/IEC 2382-37: 2022.

identity document template means a model representation of a particular identity document that is used to verify an acquired image of an identity document of that type.

Example: The identity document template may include, but is not limited to, text locations, colours and other graphical elements, security features, and locations of facial biometric information for identity documents that are also photo IDs.

in-device biometric capability means the built-in biometric capability provided by original equipment manufacturers for smartphones, including the biometric sensor, the presentation attack detection subsystem, and the biometric matching algorithm.

Example: Capabilities provided by online equipment manufacturers for smartphones include FaceID or Fingerprint Unlock.

ISO/IEC 17025:2017 means the standard for general requirements for the competence of testing and calibration laboratories, published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/66912.html.

ISO/IEC 19795-2:2007 means Part 2 (concerning testing methodologies for technology and scenario evaluation) of the series of standards designated

ISO/IEC 19795 (concerning biometric performance testing and reporting), published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/41448.html.

ISO/IEC TS 19795-9:2019 means Part 9 (concerning testing on mobile devices) of the series of standards designated ISO/IEC TS 19795 (concerning biometric performance testing and reporting), published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/78101.html.

ISO/IEC 2382-37:2022 means Part 37 (concerning biometrics) of the series of standards designated ISO/IEC 2382 (concerning vocabulary), published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/73514.html.

ISO/IEC 24745:2022 means the standard for biometric information protection, published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/75302.html.

ISO/IEC 30107-1:2023 means Part 1 (concerning framework) of the series of standards designated ISO/IEC 30107 (concerning biometric presentation attack detection), published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/83828.html.

ISO/IEC 30107-3:2023 means Part 3 (concerning testing and reporting) of the series of standards designated ISO/IEC 30107 (concerning biometric presentation attack detection), published by the International Organization for Standardization.

Note: At the time this instrument was made, located at https://www.iso.org/standard/79520.html.

ISP means an accredited identity service provider.

look-up secret means a physical or electronic record that stores a set of secrets shared between an individual and the accredited entity authorised to provide an authenticator service.

memorised secret means a secret value chosen and memorised by the individual, such as a password or PIN.

MF crypto device is short for multi-factor cryptographic device.

MF crypto software is short for multi-factor cryptographic software.

MF OTP device is short for multi-factor one-time password device.

Section 1.4

MitM means a man-in-the-middle attack whereby an adversary intercepts communications between 2 parties and presents themselves to each party as if the adversary were the other party.

multi-factor cryptographic device means a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor.

Note: Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software on the hardware device is under the effective control of the accredited entity providing authentication services.

multi-factor cryptographic software means a cryptographic key that is stored in some form of removable media or device that requires activation through a second authentication factor.

multi-factor one-time password device means a device that generates OTPs as part of an authentication activity.

Note: This includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The OTP is displayed on the device and input or transmitted by an individual, proving possession and effective control of the device.

one-time password means a password that is only valid for a single authentication event.

OTP is short for one-time password.

out-of-band device means a physical device that uses an alternative channel for transmitting information.

phishing resistance means authentication methods implemented by an accredited entity for preventing and addressing impersonation attacks.

presentation attack instrument species means a class of presentation attack instrument created using a common production method and based on different biometric characteristics.

PSTN means public switched telephone network.

reauthentication means the process by which the accredited entity reconfirms that a session is still under the control of the individual.

replay resistance means protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorised effect or gaining unauthorised access.

second-generation document image means a digital or printed image of a reproduced (for example, photocopied, scanned, or photographed) unedited genuine document.

SF crypto device is short for single-factor cryptographic device.

SF crypto software is short for single-factor cryptographic software.

SF OTP device is short for single-factor one-time password device.

single-factor cryptographic device means a hardware device that performs cryptographic operations using one or more protected cryptographic keys and authenticated by proving possession and effective control of the cryptographic key.

single-factor cryptographic software means a cryptographic key that is stored in some form of soft media.

single-factor one-time password device means a device that generates and displays OTPs, including hardware devices, SMS or software-based OTP generators installed on devices such as mobile phones.

1.5 Incorporated instruments

If a provision of this instrument applies, adopts or incorporates, with or without modification, any matter contained in any other instrument or other writing (***incorporated instrument***), then the reference to the incorporated instrument is as in force at the commencement of this instrument.

1.6 Application—transitioned accredited entities

(1) Paragraph (b) in column 2 of item 3 of the table in section 3.13 applies to a transitioned accredited entity starting on the day that is 12 months after the day on which this instrument commences.

(2) Every provision of this instrument not specified in subsection (1) applies to a transitioned accredited entity in accordance with its terms and on and from the commencement of this instrument.

Section 2.1

Chapter 2—Data standards for ISPs

Part 1—Biometric testing

2.1 Definitions

In this Part:

document false accept rate means the proportion of document verification transactions with credential fraud that are incorrectly confirmed as authentic.

document false reject rate means the proportion of genuine document verification transactions with truthful claims of a genuine document that are incorrectly denied.

document fraud attack means the techniques used to create fraudulent documents.

Note: Techniques can be digital or physical and can include document tampering or creation of a counterfeit document.

document fraud instrument means an object or image used in a credential fraud attack.

Example: A forged or counterfeit photo ID.

document fraud instrument species means a class of document fraud instruments created using a common production method and based on different persons.

FIDO document authenticity verification requirements means the requirements developed by the FIDO (Fast Identity Online) Alliance for testing eIDVT solutions.

Note: At the time this instrument was made, located at https://fidoalliance.org/specs/idv/docauth/document-authenticity-verification-requirements-v1.0-fd-20220815.html.

test set has the same meaning as in section 6.2 of the FIDO document authenticity verification requirements.

2.2 Biometric testing entity

(1) Biometric testing must be conducted by a person that:
  (a) uses personnel experienced in conducting biometric testing;
  (b) is, or uses, a laboratory accredited against ISO/IEC 17025:2017 that is certified for the assessment of biometric technology testing standards;
  (c) has, and applies, a policy for working with human test subjects that has been approved by a relevant national body;
  (d) has established test methods for:
    (i) presentation attack detection testing informed by ISO/IEC 30107-3:2023, if conducting testing of presentation attack detection technology; and

(ii) testing of accuracy of the biometric matching algorithm informed by ISO/IEC 19795-2:2007, if conducting testing of a biometric matching algorithm; and

(e) is independent from the design, implementation, operation and management of the accredited entity's accredited services and DI data environment and is:

(i) external to the entity; or

(ii) if the entity is part of a group, external to the group.

Note 1: An ISP that conducts authentication using biometric information using custom biometric capability must ensure its presentation attack detection technology is tested by a biometric testing entity—see item 4 in the table in section 3.13.

Note 2: For paragraph (d), a person accredited to conduct presentation attack detection testing according to ISO/IEC 30107-3:2023 and/or biometric performance testing according to ISO/IEC 19795-2:2007 under the National Voluntary Laboratory Accreditation Program coordinated by the National Institute of Standards and Technology ordinarily would meet the requirements in that paragraph.

Note 3: For testing of eIDVT, the biometric testing entity must also meet subsection 2.7(2).

(2) A person that meets all the requirements in subsection (1) is a ***biometric testing entity***.

2.3 Testing of presentation attack detection technology

(1) In this section:

level A presentation attack instrument species means a category of presentation attack instruments which:

(a) have an elapsed creation time equal to or less than one day;

(b) can be created or undertaken by a layperson;

(c) can be undertaken with standard equipment; and

(d) involve a source of biometric information which is easy to obtain such as a photo from social media or a voice recording.

level B presentation attack instrument species means a category of presentation attack instruments which:

(a) have an elapsed creation time equal to or less than 7 days;

(b) can be created or undertaken by a person who has the required expertise to do so;

(c) can be undertaken with standard or specialised equipment; and

(d) involve a source of biometric information which is moderately difficult to obtain such as a stolen fingerprint image or a voice recording of a specific phrase.

General requirement

(2) Where an ISP conducts online biometric binding, its presentation attack detection technology and liveness detection must be tested by a biometric testing entity in accordance with the requirements specified in ISO/IEC 30107-3:2023 and this Part.

Section 2.3

Additional requirements for testing of presentation attack detection technology

(3) Testing of presentation attack detection technology must be conducted in accordance with the standards in the following table.

Standards for testing of presentation attack detection technology

Item	For:	the standard is:
1	the testing:	must comply with the following: (a) be conducted on a system that incorporates all hardware and software involved in the ISP's biometric binding process; (b) be conducted using configurations and settings that align to the ISP's DI data environment; (c) calculate and record the completed presentation attack detection evaluation and corresponding results for each presentation attack instrument species as those artefacts and process for testing are defined by ISO/IEC 30107-3:2023, and this section; (d) include presentation attack instrument species to address potential presentation attack threats to the presentation attack detection technology and mechanism for liveness detection, as informed by the ISP's cyber security risk assessment and fraud risk assessment; (e) include at least 6 level A presentation attack instrument species and at least 6 level B presentation attack instrument species; and (f) include a minimum of 10 individuals.
2	each presentation attack instrument species:	must create at least one presentation attack instrument covering a minimum of 3 individuals and must be included in the testing.
3	presentation attack instrument species used in testing:	(a) must meet the requirement for an APCER of 0%; (b) however, if the reported APCER for any presentation attack instrument species does not meet the requirement in paragraph (a), the biometric testing entity must: (i) conduct supplementary testing of any presentation attack instrument species that failed to meet the requirement in paragraph (a); and (ii) subject to paragraph (c), confirm that the supplementary testing concluded that the presentation attack instrument species successfully met the requirement in paragraph (a); (c) if up to one level B presentation attack instrument species used in the testing has an APCER equal to or less to 5%, with all other level B and level A presentation attack instrument species having an APCER of 0%, the biometric testing entity must include in its report to the ISP a risk rating and recommended mitigation strategies. Note: For custom biometric capability, APCER must be no more than 10%—see paragraph (k) of item 4 in the table in section 3.13.

Standards for testing of presentation attack detection technology		
Item	**For:**	**the standard is:**
4	the testing report and ISP's response:	(a) the ISP must: (i) obtain a copy of the testing report from the biometric testing entity; and (ii) ensure the report confirms that the ISP's presentation attack detection technology has been tested in accordance with ISO/IEC 30107-3:2023 and this Part; and (b) if paragraph (c) of item 3 applies, the ISP must respond in writing to the findings and recommendations in the report as required by section 2.4.

2.4 ISP's response to testing report

For item 4 in the table in section 2.3, the ISP's response to the testing report must include:

(a) for each finding and recommendation in the report:
  (i) a risk matrix based on an established risk management framework;
  (ii) a risk assessment;
  (iii) a risk rating in accordance with its risk matrix;
  (iv) a response to each risk identified in the report as requiring treatment; and
  (v) a response to each recommendation in the report; and

(b) for each risk and recommendation accepted by the ISP:
  (i) details of the action the ISP will take to implement the treatment or recommendation;
  (ii) the timeframe in which the ISP will complete the action, having regard to the risk rating assigned for the risk or recommendation; and
  (iii) the residual risk rating expected following completion of the action; and

(c) for each risk and recommendation not accepted by the entity:
  (i) the reasons for the non-acceptance;
  (ii) details of alternative actions, if any, to be taken by the entity and the timeframes to do so; and
  (iii) the residual risk rating expected following implementation of any alternative action.

2.5 Testing of biometric matching algorithm

(1) For biometric testing of technical biometric matching and eIDVT, the biometric matching algorithm must be tested by a biometric testing entity in accordance with the testing and reporting specifications described in ISO/IEC 19795-2:2007 to determine the:
  (a) failure to enrol rate;
  (b) failure to acquire rate;
  (c) false match rate; and

(d) false non-match rate.

(2) The biometric matching algorithm must:

(a) be tested using operational configurations and settings that are consistent with and align to the ISP's operating environment;

(b) be tested having regard to the range of individuals who may be potential users of the ISP's accredited services;

(c) be tested using representation from a diverse range of individuals mentioned in paragraph (b), including:

(i) individuals with disability; and

(ii) individuals with a diverse range of ability, including ability to use technology; and

(iii) individuals with a diverse range of age, gender and ethnicity; and

(d) establish, with a minimum 90% confidence interval, that the algorithm achieves a false match rate of not more than 0.01% and a false non-match rate of not more than 3%, as described in ISO/IEC TS 19795-9:2019.

2.6 Testing of source biometric matching

For biometric testing of source biometric matching, the ISP must conduct end-to-end testing to ensure:

(a) the entity's biometric capability, including the image quality profile requirements, meets the requirements of the:

(i) authoritative source; or

(ii) service that confirms the veracity of information with an authoritative source; and

(b) the source biometric matching works as a repeatable process.

2.7 Testing of eIDVT

(1) In this section:

level A, ***level B*** or ***level C***, in relation to document fraud attacks, have the meanings for each of those levels in section 6.2.1.2 of the FIDO document authenticity verification requirements.

(2) Where biometric testing is of an ISP's eIDVT, the biometric testing entity conducting the testing must:

(a) be a FIDO Accredited Laboratory as defined by the FIDO document authenticity verification requirements;

(b) use personnel experienced in eIDVT testing; and

(c) have, and implement, policy and procedures that demonstrate responsible management and storage by the biometric testing entity of physical document fraud instruments.

FIDO document authenticity verification requirements

(3) The eIDVT must be tested according to, and meet the requirements of:

(a) subject to paragraph (b)—rule 5.20 of the Accreditation Rules;

(b) in relation to paragraph 5.20(4)(b) of the Accreditation Rules—the standards in the table in subsection (4);
(c) the FIDO document authenticity verification requirements; and
(d) the additional requirements to the FIDO document authenticity verification requirements in the following table.

Additional requirements to the FIDO document authenticity verification requirements

Item	FIDO section:	the additional requirement is:
1	Section 6.2 (test sets):	must be reasonably balanced across document types and contain at least 30 of each listed document type supported by the eIDVT.
2	Section 7.2.2 (test crew and associated genuine documents):	the test set for physical document testing: (a) are to be reasonably balanced across document types and must contain at least 10 of each listed document supported by the eIDVT; and (b) the eIDVT must meet the criteria described in 3.1 of the FIDO document authenticity verification requirements (performance levels), but must achieve a document false reject rate of 1% or below and the document false accept rate of 1%, for both digital testing and physical document testing.

Standards for eIDVT testing for document liveness

(4) When conducting eIDVT testing, the standards in the following table apply.

Standards for eIDVT testing for document liveness requirements

Item	Requirement:	the standard is:
1	Inputs for digital document testing—for digital document testing:	the ISP must use: (a) 300 images of documents for each test set (see section 6.2 of the FIDO document authenticity verification requirements); or (b) 300 instances of the inputs the eIDVT uses to detect document liveness that include, but are not limited to, the following: (i) short video; (ii) two or more separate images either at different angles or of the reverse of the document; or (iii) another challenge or response as required by the technical specifications of the eIDVT testing.
2	The images referred to in item 1:	must reasonably cover: (a) varying geographics for document types the entity accepts for eIDVT biometric matching; and (b) for demographics represented on the images of the documents, a diverse range of individuals, including individuals with disability and individuals with a diverse range of age, gender, ability and ethnicity.

Section 2.7

Standards for eIDVT testing for document liveness requirements		
Item	**Requirement:**	**the standard is:**
3	Levels of document fraud attacks in scope for digital document testing:	the following levels of document fraud attack for digital document testing of document fraud instruments are within scope: (a) level A attacks; (b) level B attacks; and (c) level C attacks.
4	Evaluations with document fraud instruments in digital testing—the test set of document fraud instruments used for digital document testing:	must: (a) comply with the conditions imposed by section 6.3.2 of the FIDO document authenticity verification requirements; and (b) contain: (i) at least 10% of document fraud instruments at level A, B, and C that are genuine second-generation document images; and (ii) no documents that are considered to be out-of-scope for processing through the eIDVT.
5	Levels of document fraud attacks in scope for physical testing:	the following levels of document fraud attack for physical testing of document fraud instruments are within scope: (a) level A attacks; and (b) level B attacks.
6	Test set conditions for physical evaluation using document fraud instruments:	must include: (a) minimum of 100 document fraud instruments which reasonably include: (i) varying geographics for document types the entity accepts for eIDVT biometric matching; and (ii) for demographics represented on the images of the documents, a diverse range of individuals, including individuals with disability and individuals with a diverse range of age, gender, ability and ethnicity; (b) only document fraud instruments that are reproduced forms of genuine documents being printed versions of second-generation document images; (c) no physically tampered documents; (d) at least 30% document fraud instruments at level A representing at least 3 or more document fraud instrument species; (e) at least 30% document fraud instruments at level B representing at least 3 or more document fraud instrument species; and (f) no document types that are considered out-of-scope for processing through the eIDVT.
7	Document verification transactions with physical document fraud instruments:	the biometric testing entity must conduct testing with physical document fraud instruments according to the rules for transactions for testing for genuine physical documents as set out in section 7.3.1 of FIDO document authenticity verification requirements.

Standards for eIDVT testing for document liveness requirements		
Item	**Requirement:**	**the standard is:**
8	Metrics to be calculated for physical document fraud instruments:	the document false accept rate must be calculated in accordance with section 3.1.2 of FIDO document authenticity verification requirements.

(5) The ISP must ensure:

(a) the biometric testing entity provides it with a report; and

(b) the biometric testing entity's report confirms that the ISP's eIDVT has been tested in accordance with the requirements in this section.

(6) The ISP must maintain a list of the unique kinds of credentials accepted by the eIDVT for verification and the list must include:

(a) the kind of credential;

(b) the issuer of the credential; and

(c) the series or version of the kind of credential.

Note: See Schedules 1 to 4 in the Accreditation Rules for kinds of credentials.

(7) If new kinds of credentials are included in the ISP's eIDVT for verification, the eIDVT must be retested in accordance with this section for those credentials.

Part 2—Authenticating to a digital ID

Division 1—Authentication levels

3.1 Authentication levels: AL Table

The following table (***AL Table***):

(a) specifies 3 authentication levels (AL1, AL2 and AL3);

(b) the kinds of authenticators that can be used for each authentication level (item 1);

(c) reauthentication requirements for each authentication level (item 2);

(d) mandatory security requirements for each authentication level (items 3 to 7), where 'must' stated in the column for the authentication level means the requirement is mandatory for that authentication level; and

(e) the allowed combinations of authentication levels and identity proofing levels (item 8).

AL Table

Item	Column 1	Column 2	Column 3	Column 4
	Requirement	**AL1**	**AL2**	**AL3**

1	**Kinds of authenticators**	One of the following:
		• memorised secret;
		• look-up secret;
		• SF OTP device;
		• SF crypto software;
		• SF crypto device;
		• MF OTP device;
		• MF crypto software;
		• MF crypto device.
			One of the following:
			• MF OTP device;
			• MF crypto software;
			• MF crypto device; or
			• a memorised secret and one the following:
			  ○ look-up secret;
			  ○ out-of-band device;
			  ○ SF OTP device;
			  ○ SF crypto software;
			  ○ SF crypto device.
				One of the following:
				• MF crypto device;
				• SF crypto device and memorised secret;
				• SF OTP device and MF crypto software;
				• SF OTP device and MF crypto device;
				• SF OTP device and SF crypto software and memorised secret.

2	**Reauthentication**	Where the authenticated session is persistent, the individual must reauthenticate to their digital ID after 30 days.	Where the authenticated session is persistent, the individual must reauthenticate to their digital ID after 12 hours, regardless of	Where the authenticated session is persistent, the individual must reauthenticate to their digital ID after 12 hours, regardless

AL Table				
Item	**Column 1**	**Column 2**	**Column 3**	**Column 4**
	Requirement	**AL1**	**AL2**	**AL3**
		For reauthentication, the individual must use at least 1 authentication factor.	user activity. Otherwise, the session must be terminated. After 30 minutes of inactivity, the individual must reauthenticate to their digital ID. Otherwise, the session must be terminated. For reauthentication, the individual must use at least 1 authentication factor. For reauthentication, the individual must use a memorised secret or authentication using biometric information.	of user activity. Otherwise, the session must be terminated. After 15 minutes of inactivity, the individual must reauthenticate to their digital ID. Otherwise, the session must be terminated. For reauthentication, the individual must use both authentication factors.
	Security			
3	MitM resistance	Must	Must	Must
4	Phishing resistance	—	—	Must
5	AE-compromise resistance	—	—	Must
6	Replay resistance	—	Must	Must
7	Authentication intent	—	—	Must
8	AL level to be combined with an identity proofing level	IP1	Identity proofing levels up to and including IP3.	All identity proofing levels

Division 2—Binding authenticators to a digital ID

3.2 Binding an authenticator when generating a digital ID

(1) For remote transactions where generating the digital ID and binding of the authenticator to that digital ID cannot be completed in a single electronic transaction that is a single protected session:

(a) individuals must identify themselves in the binding transaction by presenting a temporary secret which was either established during a prior transaction or sent to the individual's mobile phone number or email address (***temporary secret***); and

(b) long-term authentication secrets must be issued to an individual only within a protected session.

Note: Generating the digital ID and binding of the authenticator may not be completed in a single electronic transaction that is a single protected session where the identity proofing is conducted online and the individual is required to collect a physical item such as a lookup secret.

(2) For in-person transactions where the generation of the digital ID and binding of an authenticator to that digital ID cannot be completed in a single physical encounter within a single protected session:

(a) individuals must identify themselves in-person by either presenting a temporary secret, or by biometric authentication;

(b) temporary secrets must not be reused; and

(c) if the ISP issues long-term authentication secrets during an in-person transaction, those secrets must be loaded locally on to a physical device that is issued in-person to the individual or delivered in a manner that confirms the individual's email address or mobile phone number.

Division 3—Standards for kinds of authenticators

3.3 Memorised secrets

For memorised secrets, the standards in the following table apply.

Standards for memorised secrets		
Item	**Requirements—If:**	**the standard is:**
1	a memorised secret is chosen by an individual:	must be at least 8 characters long.
2	a memorised secret is chosen randomly by the accredited entity:	must be at least 6 characters long and may be entirely numeric.
3	a request from an individual is being processed to establish or change a memorised secret:	the ISP must compare the prospective secret against a list that contains secrets known to be commonly used, expected or compromised. Example: The list may include: • passwords obtained from previous breach corpuses; • dictionary words; • repetitive or sequential characters (e.g. “aaaaaa”, “1234abcd”); and • context-specific words, such as the name of the service, the username, and derivatives thereof.
4	the chosen secret is found in the list referred to in item 3:	the ISP must: (a) notify the individual that they need to select a different secret; (b) provide the reason for rejection; and (c) require the individual to choose a different secret.
5	a memorised secret is being requested:	the ISP’s information technology system must use an AACA and an authenticated protected channel.
6	a memorised secret is being stored:	must be stored in a form that is resistant to offline attacks, including by ensuring: (a) memorised secrets are salted and hashed using a suitable one-way cryptographic key derivation function; (b) the salt value is at least 32 bits in length and be chosen arbitrarily so as to minimise salt value collisions among stored hashes; and (c) both the salt value and the resulting hash are stored for each individual who uses memorised secrets.

Section 3.4

3.4 Look-up secrets

For look-up secrets, the standards in the following table apply.

Standards for look-up secrets

Item	Requirements—If:	the standard is:
1	a look-up secret is delivered to an individual:	must be delivered in a secure manner.
2	a look-up secret is requested from the individual:	the individual must be prompted for the next secret from the individual's authenticator or for a specific secret.
3	a look-up secret is given to an individual:	must only be used successfully once.
4	the lookup secret is derived from a grid card:	each cell of the grid must be used only once.
5	a look-up secret is stored:	must be stored in a form that is resistant to offline attacks, including by ensuring: (a) look-up secrets are hashed using an AACA; and (b) for look-up secrets that have less than 112 bits of entropy—the look up secret is salted before being hashed with a salt value that is at least 32 bits in length and arbitrarily chosen so as to minimise salt value collisions among stored hashes.
6	an individual uses look-up secrets:	must store both the salt value and the resulting hash for each individual referred to in item 5.
7	the ISP requests a look-up secret to provide resistance to eavesdropping and MitM:	must use an AACA and an authenticated protected channel.

3.5 Single-factor one-time password devices

For single-factor one-time password devices, the standards in the following table apply.

Standards for single-factor one-time password devices

Item	Requirement	the standard is:
1	For the secret cryptographic key and its algorithm:	must provide the minimum-security strength specified in the ISM's Guidelines for Cryptography relevant to the AACA in use.
2	For the nonce:	must be of sufficient length to ensure that it is unique for each operation of the device over its lifetime. Note: The specific secret may be, for example, the next numbered secret.
3	If the nonce used to generate the authentication output is based on a real time clock:	the nonce must be changed at least once every 2 minutes.
4	The OTP value associated with a given nonce:	must not be accepted more than once.

Standards for single-factor one-time password devices		
Item	**Requirement**	**the standard is:**
5	If a single-factor OTP authenticator is being associated with a digital ID:	must use an AACA to either generate and exchange, or to obtain, the secrets required to duplicate the authentication output.
6	If collecting the OTP to provide resistance to eavesdropping and MitM:	must use AACAs and an authenticated protected channel.
7	If providing replay resistance, the entity's information technology system:	must not accept a given time-based OTP more than once during the validity period of the authenticator involved.
8	Time-based OTPs:	must have a defined lifetime that is determined by the expected clock drift, in either direction, of the authenticator over its lifetime, plus allowance for network delay and individual entry of the OTP.

3.6 Multi-factor one-time password devices

For multi-factor one-time password devices, the standards in the following table apply.

Note: When using biometric information as a factor for multi-factor one-time password devices, section 3.13 applies.

Standards for multi-factor one-time password devices		
Item	**Requirements:**	**the standard is:**
1	The secret cryptographic key and its algorithm:	must provide at least the minimum-security strength specified in the ISM's Guidelines for Cryptography relevant to the AACA in use.
2	The nonce:	must be of sufficient length to ensure that it is unique for each operation of the device over its lifetime.
3	The OTP authentication:	must: (a) not facilitate the cloning of the secret cryptographic key on to multiple devices; and (b) establish that the MF OTP authenticator is a MF OTP device.
4	If the nonce used to generate the authentication output is based on a real-time clock:	the nonce must be changed at least once every 2 minutes.
5	If a memorised secret is used for activation:	must be a randomly chosen numeric secret at least 6 decimal digits in length.
6	The unencrypted key and activation secret:	must be zeroised immediately after an OTP has been generated.
7	If the ISP collects biometric information using a custom biometric capability, the biometric sample, and any	must be zeroised immediately after an OTP has been generated.

Standards for multi-factor one-time password devices

Item	Requirements:	the standard is:
	biometric information derived from the biometric sample:	
8	If an MF OTP authenticator is being associated with a digital ID:	must use an AACA to either generate and exchange, or to obtain, the secrets required to duplicate the authentication output.
9	If collecting the OTP to provide resistance to eavesdropping and MitM:	must use an AACA and an authenticated protected channel when collecting the OTP.
10	Time-based OTPs:	must have a defined lifetime that is determined by the expected clock drift - in either direction - of the authenticator over its lifetime, plus allowance for network delay and individual entry of the OTP.
11	Replay resistance:	the accredited entity's information technology system must not accept a given time-based OTP more than once during the validity period of the authenticator.

3.7 Single-factor cryptographic software

For single-factor cryptographic software, the standards in the following table apply.

Standards for single-factor cryptographic software

Item	Requirement:	the standard is:
1	The secret cryptographic key and its algorithm:	must: (a) provide at least the minimum-security strength specified in the latest edition of the ISM; (b) be stored in suitably secure storage available to the authenticator application. Applications must utilise one of the following mechanisms to be considered as secure storage: (i) keychain storage; (ii) Trusted Platform Module; (iii) Trusted Execution Environment; (iv) secure element; and (c) only be accessible to the authenticating software on the device that is authorised. All unauthorised software must not be able to access the secret key.
2	The single-factor cryptographic device:	must encapsulate one or more secret cryptographic keys, unique to the device, that cannot be removed from the device.
3	The secret cryptographic key and its algorithm:	must provide at least 112 bits of effective security strength.
4	The challenge nonce:	must: (a) be at least 64 bits in length; and

Standards for single-factor cryptographic software		
Item	**Requirement:**	**the standard is:**
		(b) either be unique over the authenticator's lifetime, or be statistically unique.
5	Approved cryptography:	must be used for authentication events.
6	Cryptographic keys:	must be protected against modification and unauthorised disclosure.

3.8 Multi-factor cryptographic software

For multi-factor cryptographic software, the standards in the following table apply.

Note: When using biometric information as a factor for multi-factor cryptographic software, section 3.13 applies.

Standards for multi-factor cryptographic software		
Item	**Requirement:**	**the standard is:**
1	The secret cryptographic key and its algorithm:	(a) must only be accessible by a device's software components that require access; and (b) the ISP must implement access controls to prevent unauthorised access to the secret cryptographic key.
2	Authentication events:	must require the input of 2 or more authentication factors to execute that authentication event.
3	Any memorised secret used for activation:	must be a randomly chosen numeric value at least 6 decimal digits in length.
4	The unencrypted key and activation secret:	must be zeroised immediately after an authentication has taken place.
5	If the ISP collects biometric information using a custom biometric capability, the biometric sample, and any biometric information derived from the biometric sample:	must be zeroised immediately after an authentication has taken place.
6	Cryptographic keys:	must: (a) be stored in suitably secure storage available to the authenticator application. Applications must utilise one of following mechanism to be considered as secure storage: (i) keychain storage; (ii) Trusted Platform Module; (iii) Trusted Execution Environment; (iv) secure element; and (b) must be protected against modification; and unauthorised disclosure.

Standards for multi-factor cryptographic software		
Item	**Requirement:**	**the standard is:**
7	The challenge nonce:	must: (a) be at least 64 bits in length; and (b) either be unique over the authenticator's lifetime or be statistically unique.
8	The authentication event:	must use approved cryptography.

3.9 Multi-factor cryptographic devices

For multi-factor cryptographic devices, the standards in the following table apply.

Note: When using biometric information as a factor for multi-factor cryptographic device, section 3.13 applies.

Standards for multi-factor cryptographic devices		
Item	**Requirement:**	**the standard is:**
1	The secret cryptographic key and its algorithm:	must: (a) provide at least the minimum-security strength specified in the ISM's Guidelines for Cryptography relevant to the AACA in use; and (b) be accessible only through the presentation and verification of an activation factor, using either biometric information for authentication or an activation secret.
2	The challenge nonce:	must: (a) be at least 64 bits in length; and (b) either be unique over the authenticator's lifetime, or be statistically unique.
3	Approved cryptography:	must be used for authentication events.
4	Cryptographic keys:	must be protected against modification and unauthorised disclosure.

3.10 Single-factor cryptographic devices

For single-factor cryptographic devices, the standards in the following table apply.

Standards for single-factor cryptographic devices		
Item	**Requirement:**	**the standard is:**
1	The secret cryptographic key and its algorithm:	must: (a) provide at least the minimum-security strength specified in the ISM's Guidelines for Cryptography relevant to the AACA in use; and (b) be designed so as to prohibit the export of the authentication secret.
2	The challenge nonce:	must: (a) be at least 64 bits in length; and (b) either be unique over the authenticator's lifetime, or be statistically unique.
3	Approved cryptography:	must be used for authentication events.
4	Cryptographic keys:	must be protected against modification and unauthorised disclosure.
5	Cryptography device:	must be a separate piece of hardware or an embedded processor or execution environment.

3.11 Out-of-band devices

For out-of-band devices, the standards in the following table apply.

Standards for out-of-band devices		
Item	**Requirement:**	**the standard is:**
1	The out-of-band device:	must establish a separate channel with the ISP's information technology system to retrieve the out-of-band secret or authentication request. Note: This separate channel is out-of-band with respect to the primary communication channel (even if it terminates on the same device), provided the device does not leak information from one channel to the other without the consent of the individual.
2	The out-of-band device:	must uniquely authenticate itself in one of the following ways when communicating with the entity's information technology system: (a) establish an authenticated protected channel to the entity's information technology system that: (i) uses approved cryptography; and (ii) stores relevant cryptographic keys in suitably secure storage available to the authenticator application; or (b) only where a secret is being sent from the entity's information technology system to the out-of-band device via the PSTN, authenticate to a public mobile telephone network using a SIM card or equivalent that uniquely identifies the device.

Section 3.11

Standards for out-of-band devices		
Item	**Requirement:**	**the standard is:**
3	If the out-of-band device sends an approval message over the secondary communication channel, rather than by the individual transferring a received secret to the primary communication channel, the device:	(a) must accept transfer of the secret from the primary channel, which secret must be sent to the entity's information technology system over the secondary channel to associate the approval with the authentication transaction; or (b) must: (i) present a secret received via the secondary channel from the entity's information technology system; Example: The individual may perform the transfer manually or use a technology such as a barcode or QR code to affect the transfer. (ii) prompt the individual to verify the consistency of that secret with the primary channel, before accepting a yes/no response from the individual; and (iii) send that response to the entity's information technology system.
4	If out-of-band verification is conducted using a secure application on a device and the entity's information technology system sends a push notification to that device:	(a) the entity's information technology system must wait for the establishment of an authenticated protected channel and must verify the device's identifying cryptographic key; and (b) the identifying cryptographic key received must not be stored.
5	The entity's information technology system:	must: (a) use a verification method to uniquely identify the device; and (b) authenticate the device before transmitting the authentication secret to the device.
6	The entity's information technology system;	must, depending on the type of out-of-band device: (a) transfer the secret to the primary channel as follows: (i) signal the device containing the individual's authenticator to indicate readiness to authenticate; (ii) after transmitting such signal, transmit a random authentication secret to the out-of-band device; and (iii) wait for the random authentication secret to be returned on the primary communication channel; or (b) transfer the secret to the secondary channel as follows: (i) display a random authentication secret to the individual via the primary channel; and (ii) wait for the random authentication secret to be returned on the secondary channel from the individual's out-of-band device; or (c) obtain verification of secrets from the individual as follows:

Standards for out-of-band devices		
Item	**Requirement:**	**the standard is:**
		(i) displays a random authentication secret to the individual via the primary channel; (ii) sends the same random authentication secret to the out-of-band device via the secondary channel for presentation to the individual; and (iii) after transmitting the random authentication secret referred to in subparagraphs (c)(i) and (ii), wait for an approval (or disapproval) message via the secondary channel; and (d) for each option in this item, the authentication must be considered invalid if each of the required activities are not completed within 10 minutes.
7	To provide replay resistance:	the entity's information technology system must not accept a given authentication secret more than once during the validity period.
8	Random authentication secrets:	must have with at least 20 bits of entropy.
9	If the random authentication secret has less than 64 bits of entropy:	the entity's information technology system must incorporate a rate-limiting mechanism that limits the number of failed attempts to authenticate to a digital ID.
10	If out-of-band verification is to be made using the PSTN:	the ISP must: (a) verify that the pre-registered telephone number being used is associated with a specific physical device; and (b) conduct the verification in accordance with the risk-management strategies required to be detailed in the entity's system security plan (see Subdivision 1 of Division 3 of Part 4.1 of Chapter 4 of the Accreditation Rules); (c) inform individuals in clear and simple terms of the security risks of using out-of-band verification via the PSTN; and (d) offer individuals at least one alternative authenticator that can be used to authenticate to the required authentication level.
11	Out-of-band verification:	must not use email or voice-over-IP (VOIP) telephone numbers.
12	If an individual requests to change their pre-registered telephone number:	the individual must first authenticate to their digital ID using their existing authenticator.

Division 4—Standards for security requirements

3.12 Standards for security requirements

When authenticating an individual to their digital ID, the standards in the following table apply.

Standards for security requirements

Item	Requirements:	the standard is:
1	Phishing resistance (when authenticating to AL3):	(a) an authenticator is not phishing resistant if it involves the manual entry of an authentication output, such as out-of-band and OTP authenticators; (b) the phishing resistant authentication protocol must: (i) establish an authenticated protected channel with the entity's information technology system; and (ii) strongly and irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authentication output; Note: The binding may occur by signing the 2 values together using a private key (the cryptographic key in an asymmetric cryptographic key pair that must be kept secret) controlled by the individual for which the public key is known to the entity. (c) the ISP's information technology system must validate the signature or other information used to prove phishing resistance; (d) an AACA must be used to establish phishing resistance; and (e) cryptographic keys for the purpose of establishing phishing resistance must provide at least 112 bits of effective security strength.
2	AE-compromise resistance when authenticating to AL3:	(a) public keys stored by the ISP must be associated with the use of an AACA; and (b) cryptographic keys must provide at least 112 bits of effective security strength.
3	Authentication intent:	when authenticating to AL3, and AL2 if authentication intent is used for that level, the authentication intent must be established by the authenticator itself.

Standards for security requirements		
Item	**Requirements:**	**the standard is:**
4	Rate limiting (throttling):	(a) rate limiting must be implemented and maintained for each of: (i) memorised secrets; (ii) look-up secrets; (iii) single-factor OTPs; and (iv) multi-factor OTPs; (b) controls must be implemented and maintained within the entity's information technology system to protect authenticators against online guessing attacks; and (c) consecutive failed authentication attempts on the digital ID of an individual must be limited to no more than 100.
5	Authenticator attestation where the authenticator attestation is signed:	the attestation must be signed using a digital signature that provides at least 112 bits of effective security strength.

Division 5—Authentication using biometric information

3.13 Standards for authentication using biometric information

When authenticating an individual to their digital ID using biometric information of the individual, the standards in the following table apply.

Standards for authentication using biometric information

Item	Column 1 Requirement:	Column 2 Requirement:
1	Use of biometric information for authentication:	must be conducted only using: (a) in-device biometric capability (see item 3 in this table); or (b) custom biometric capability (see item 4 in this table).
2	When biometric information can be used for authentication as a factor to unlock a multi-factor authenticator:	(a) only where the relevant authenticator is a: (i) multi-factor one-time password device; (ii) multi-factor cryptographic software; or (iii) multi-factor cryptographic device; and (b) only where the relevant authenticator: (i) requires 2 or more factors to execute a single authentication event; and (ii) is possession-based, where the device is authenticated as a part of the single authentication event.
3	In-device biometric capability:	must: (a) only be used as a factor for authentication events to meet AL1 or AL2; and (b) not allow the use of in-device biometric capability that operates on devices that cannot receive operating system security updates.

Standards for authentication using biometric information

Item	Column 1 Requirement:	Column 2 Requirement:
4	Custom biometric capability:	(a) an authenticated protected channel between the sensor and the accredited entity's information technology system must be set up before capturing the biometric information from the individual; (b) must use a biometric matching algorithm to conduct one-to-one biometric matching between the acquired image and the biometric template; (c) biometric matching must be conducted using the biometric matching algorithm: (i) locally on the individual's device; or (ii) centrally, being where the biometric information is transferred to the entity's information technology system and the biometric matching is conducted remotely by the entity from the individual's device; (d) if biometric matching is conducted centrally: (i) use of the biometric as an authentication factor must be limited to one or more specific devices that are identified using approved cryptography; (ii) a separate cryptographic key must be used for identifying the device, as distinct from the biometric factor; (iii) all transmission of biometrics must occur over the authenticated protected channel; and (iv) biometric template protection specified in ISO/IEC 24745:2022 must be implemented; (e) presentation attack detection must: (i) be based on data captured by both the data capture subsystem and through system level monitoring, as described by ISO/IEC 30107-1:2023; and (ii) include liveness detection; (f) the capture of the acquired image and presentation attack detection processes must be completed as part of the same process before submission of the acquired biometric for biometric matching; (g) the presentation attack detection determination (as to whether the biometric presentation passes as being genuine according to the PAD system) must be made either: (i) locally on the individual's device; or (ii) centrally (where the biometric information is transferred to the ISP's information technology system and the biometric matching is conducted remotely by the entity from the individual's device); (h) presentation attack detection must allow no more than 5 consecutive failed authentication attempts;

Section 3.13

Standards for authentication using biometric information		
Item	**Column 1** **Requirement:**	**Column 2** **Requirement:**
		(i) once the limit of consecutive failed attempts has been reached, the custom biometric capability must either: (i) impose a delay of at least 30 seconds before the individual's next attempt to authenticate using the custom biometric capability, increasing exponentially with each successive attempt (e.g., one minute before the following attempt, 2 minutes before the second following attempt); or (ii) disable the custom biometric capability for authentication and offer another authentication factor that is a different biometric modality or a PIN/passcode if not already a required factor; (j) subject to paragraph (k)—the presentation attack detection technology must be tested in accordance with section 2.3; (k) despite item 3 in the table in section 2.3 all presentation attack instrument species used in testing of the biometric algorithm must have an APCER of no more than 10%; and (l) the biometric matching algorithm must be tested in accordance with section 2.5.